REMARKS

Claims 8, 38, 42 and 43 have been canceled. Claims 1-7, 9-37, 39-41 and 44-54 are now pending in this application.

Reconsideration of the application is earnestly requested. The Examiner is thanked for the telephone interview of April 19, 2005. The reasons presented at the interview that warrant favorable action are presented below. The Examiner has rejected claims 1 and 37 under *Carrott et al.* (*Carrott*). The Examiner has also rejected claims 25 and 52 under *Carrott* in view of *Lake et al.* Although the Examiner's arguments have been carefully considered, Applicant respectfully traverses these rejections as explained below.

Carrott shows a customer 100 with a personal computer connected over a network to a merchant site 140 and a financial institution 150. For the sake of argument, assume that these entities are analogous to the presenter, acceptor and trusted party of claims 1 and 37.

Claim 1

Claim 1 requires an enrollment process in which the trusted party receives profile data from the presenter, authenticates the presenter and associates authentication data (for example, a password) with the presenter. Specifically, claim 1 requires:

receiving, by said trusted party during an enrollment process, profile data from said presenter, and

verifying, by said trusted party during said enrollment process, the authenticity of said presenter and associating authentication data with said presenter.

The advantage of the enrollment process is that the trusted party authenticates the presenter and the associated profile data such that the trusted party can later authenticate that any profile data submitted by the presenter during a transaction is authentic. The authentication data established during the enrollment process is later used by the presenter to prove that he is who he says he is.

Carrott does not disclose any such enrollment process, does not show a trusted party verifying the authenticity of a presenter during an enrollment process, and does not show establishing authentication data as required by claim 1. Prior to the actual transaction discussed in *Carrott*, there is no interaction between the customer and the financial institution, and certainly no authenticating of the customer nor the establishment of a password to be used later

during the transaction. The way that *Carrott* confirms the transaction to the merchant is simply by comparing an address submitted by the customer with an address in a database provided by a credit agency. (Column 7, first paragraph.) But, there was no prior enrollment process.

Further, claim 1 requires that during the actual online transaction that the trusted party receives authentication data from the presenter and that the trusted party then authenticate the presenter. Specifically, claim 1 requires:

receiving, at said trusted party, submitted authentication data from said presenter during said on-line transaction, and

authenticating said presenter by comparing said submitted authentication data received from said presenter with said authentication data.

The advantage of these steps is that the trusted party authenticates the presenter during the transaction and can thus vouch for the authenticity of the presenter in conjunction with the profile data that the presenter has submitted. Absent these steps, any illegitimate party could submit accurate profile data and pretend to be the presenter.

Carrott does not disclose that the financial institution authenticates the customer during the actual transaction, and certainly does not disclose that the customer sends a password to the financial institution during the transaction for purposes of authentication. *Carrott* discloses that customer information is sent from the merchant site to the financial institution for verification, but the only action the financial institution takes is to compare the address received with an address from a historical database. Nowhere is it disclosed that the financial institution engages with the customer directly to determine the customer's authenticity. (See column 6, line 62-column 7, line 39; column 2, first, second and sixth paragraphs.) For example, column 2, line 67 states: "The financial institution decrypts the customer code and returns a purchase authorization decision to the merchant over the computer network."

Because *Carrott* does not disclose these required features of an enrollment process and authentication of the presenter during the transaction, each of which renders claim 1 patentably distinct, it is requested that the rejection be withdrawn.

Claim 37

Claim 37 also requires an enrollment process in its first two steps, and authentication of the presenter by the trusted party during the on-line transaction in its fourth and fifth steps. For

the reasons given above with respect to *Carrott*, it is submitted that each of these features renders claim 37 patentable and it is requested that the rejection be withdrawn.

Further, claim 37 also requires:

querying said trusted party by said acceptor for said trusted party to provide said profile data to said acceptor; and

providing said profile data of said presenter, by said trusted party, to said acceptor.

The advantage of these steps is that a presenter need not supply all the acquired profile data to the acceptor. The acceptor queries the trusted party for the profile data and the trusted party provides the profile data to the acceptor on behalf of the presenter. Less work is required by the presenter, fewer errors occur, and the acceptor can feel more confident about the supplied profile data. Respectfully, it is submitted that *Carrott* does not disclose these steps.

Claim 25

Claim 25 also requires an enrollment process in which a trusted party associates authentication data with a presenter. The presenter submits enrollment data for authentication and profile data to be used for later comparison during and online transaction. Specifically, claim 25 requires:

a presenter who submits enrollment data and profile data to a trusted party during an enrollment process, and with whom is associated authentication data during said enrollment process; and

said trusted party who receives said enrollment data and said profile data during said enrollment process.

As noted above, *Carrott* does not disclose an enrollment process, does not disclose a presenter who submits enrollment data to a trusted party, and does not disclose that authentication data (such as a password) is associated with the presenter during the enrollment process.

Claim 25 also requires that the trusted party receives authentication data from the presenter during the actual online transaction and that the trusted party then authenticate the presenter during the online transaction. Specifically, claim 25 requires:

[a trusted party] who receives said authentication data from said presenter during an on-line transaction, and who authenticates said authentication data and validates said profile data of said presenter during said on-line transaction.

Carrott does not disclose either the enrollment process nor a trusted party authenticating a presenter during an online transaction, each of which renders claim 25 patentably distinct. Neither does *Lake* disclose a trusted party authenticating a presenter during an online transaction. *Lake* requires the use of a digital certificate that is sent from the authentication server to the cardholder's computer (see paragraphs 8 and 9). Use of a digital certificate and cryptography is more complex than the present invention that requires only authentication data (for example, a password) from the presenter. For these reasons, it is requested that the rejection be withdrawn.

Claim 52

Claim 52 also requires an enrollment process in which a trusted party associates authentication data with a presenter. The presenter submits enrollment data for authentication and profile data to be used for later comparison during and online transaction. Specifically, claim 52 requires:

a presenter who submits enrollment data and profile data to a trusted party during an enrollment process, and with whom is associated authentication data during said enrollment process; and

said trusted party who receives said enrollment data and said profile data during said enrollment process.

As noted above, *Carrott* does not disclose an enrollment process, does not disclose a presenter who submits enrollment data to a trusted party, and does not disclose that authentication data (such as a password) is associated with the presenter during the enrollment process.

Claim 52 also requires that the trusted party receives authentication data from the presenter during the actual online transaction and that the trusted party then authenticate the presenter during the online transaction. Specifically, claim 52 requires:

[a trusted party] who receives said authentication data from said presenter during an on-line transaction, and who authenticates said authentication data and provides said profile data of said presenter to an acceptor during said on-line transaction.

Carrott does not disclose either the enrollment process nor a trusted party authenticating a presenter during an online transaction, each of which renders claim 52 patentably distinct. Neither does *Lake* disclose a trusted party authenticating a presenter during an online transaction. *Lake* requires the use of a digital certificate that is sent from the authentication server to the

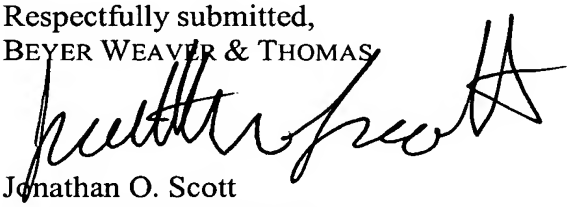
cardholder's computer (see paragraphs 8 and 9). Use of a digital certificate and cryptography is more complex than the present invention that requires only authentication data (for example, a password) from the presenter. For these reasons, it is requested that the rejection be withdrawn.

The Double Patenting Rejections

The Examiner has rejected claims 1, 2, 25 and 52 under the judicially-created doctrine of obviousness-type double patenting in view of claim 7 of U.S. application No. 09/842,313. Further, the Examiner has rejected claims 1, 2, 25 and 52 under the judicially-created doctrine of obviousness-type double patenting in view of claim 7 of U.S. application No. 10/156, 271. Accordingly, Applicant has included a terminal disclaimer pursuant to 37 C.F.R. §1.321. Applicant therefore respectfully requests that the double patenting rejection be withdrawn.

Reconsideration of this application and issuance of a Notice of Allowance at an early date are respectfully requested. If the Examiner believes a telephone conference would in any way expedite prosecution, please do not hesitate to telephone the undersigned at (612) 252-3330.

Respectfully submitted,
BEYER WEAVER & THOMAS



Jonathan O. Scott
Registration No. 39,364

BEYER WEAVER & THOMAS, LLP
P.O. Box 778
Berkeley, CA 94704-0778

Telephone: (612) 252-3330
Facsimile: (612) 825-6304